REMARKS

In the Office Action, the Examiner indicated that claims 1-6, 8-14, 16-22, and 24 are pending in the application, and claims 7, 15, and 23 have been withdrawn from consideration. The Examiner rejected all of the pending claims.

Claim Rejections, 35 U.S.C. §103

In item 2 on page 2 of the Office Action, the Examiner rejected claims 1-6, 8-14, 16-22, and 24 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,949,877 to Traw et al. ("Traw '877") in view of U.S. Patent No. 6,542,610 to Traw et al. ("Traw '610") and further in view of U.S. Patent No. 6,493,825 to Blumenau et al.

The Present Invention

The present invention allows the use of wireless devices containing a radio module to connect in a secure manner using digital certificates. The present invention does not require manual entry of user identifiers, passwords, or cryptographic keys. A private key is generated within the wireless device, and is immediately placed in *write-only storage* within the device, and cannot thereafter leave the write-only storage.

The term "write-only storage" is clearly defined in the specification, e.g., beginning on page 16, line 3. More specifically, the wireless device's private key is stored in that device using a write-only storage means, such that there is there is no way for software residing in the device to read the key but the device can execute operations against the information.

Using the "write-only storage" as defined in the specification, it is physically impossible

for its contents to be read, ever. The protected storage, being a write-only memory, is not

capable of emitting the private key value.

U.S. Patent No. 5,949,877 to Traw et al.

U.S. Patent No. 5,949,877 to Traw et al. teaches a method for protecting digital content

from copying and/or other misuse as it is transferred between devices over insecure links. The

storage of the key and the key exchange of Traw '877 is implemented in software (e.g., see Col.

3, lines 52-55; Col 4., lines 17-20). There is no teaching or suggestion of anything other than a

standard, prior art system in which the private key is in a read/write memory accessible by

software (i.e., read by the software to provide the security function of the private key).

U.S. Patent No. 6,542,610 to Traw et al.

U.S. Patent No. 6,542,610 to Traw et al. is a continuation-in-part of Traw '877 and

contains essentially the same teachings as Traw '877 with respect to storage of and access to the

private key. The Examiner appears to rely on Traw '610 for an alleged teaching of establishing

an initial session between first and second devices and negotiating a two-way session encryption

and mutual authentication requirements between the two devices.[1]

---

[1] The Examiner has repeatedly failed to identify which "Traw" reference is being referred to; Applicant cannot be sure that it has properly figured out which Traw reference is being referred to at any given point in the Office Action but has made a good-faith attempt to do so.

U.S. Patent No. 6,493,825 to Blumenau et al.

U.S. Patent No. 6,493,825 to Blumenau et al. teaches the authentication of a host

processor requesting service in a data processing network, by transmitting a random number to

an object to be authenticated. The object has an integrated circuit chip including a memory and

encryption circuitry. The memory stores information defining an encryption scheme preassigned

to the object. Blumenau discloses the use of a symmetric key (a password) that is stored in a

write-only composite chip called a "identity chip" (Figure 32, elements 361 and 363) on one

device called a "host controller". While this password is stored in the write-only identity chip,

the password also is unprotected in the cached storage subsystem port adapter memory within the

"list of keys of host controllers" (element 365 of Figure 32) to which the host controllers must

authenticate. In the system of Blumenau, if two devices need to be authenticated, or to

authenticate each other, they must know both symmetric key values beforehand, and the identity

chip protects only one of these values, that is, the identity chip protects the symmetric key value

for one of the devices.

The Examiner has not Established a *prima facie* Case of Obviousness

As set forth in the MPEP:

> To establish a *prima facie* case of obviousness, there must be some suggestion or
> motivation, either in the references themselves or in the knowledge generally
> available to one of ordinary skilled in the art, to modify the reference or to
> combine reference teachings.
> MPEP 2143

As noted above, neither of the Traw patents (Traw '877 or Traw '610) teach or suggest the use of write-only storage to store private keys in each device as defined in the present invention. The Examiner has acknowledged this fact. They simply teach traditional read/write memory used to store and access the private key. However, in contrast to the Examiner's assertion, Blumenau et al. does not teach or suggest the use of write-only storage to store private keys in each device either. As indicated above, the symmetric key or password of Blumenau is stored in an unprotected state in the cached storage subsystem port adapter memory within the list of keys of the host controllers. When two devices need to be authenticated, they must know the symmetric key value beforehand; this is why the Blumenau system leaves the symmetric key unprotected in this cached storage.

In the present invention, an asymmetric public/private key pair is used of which the private key is only known to one device and is stored on that one device in a write-only memory. There are no other copies of the private key on other devices which could be compromised, and there is no need to distribute any kind of device key to other devices before communication is initiated. When needed, the public key is sent in a certificate, but there is no need to prevent others from seeing this public value.

The write-only storage of the present invention can NEVER be read; it is impossible. This write-only storage is specifically claimed in each independent claim. The write-only storage as claimed in the present invention is patentably distinct from the disclosures of either Traw patent, as well as from Blumenau, alone or in combination. Nothing in either Traw patent, nor Blumenau, teaches or suggests the claimed invention.

Each of the independent claims of the present invention specifically recites the write-only

storage as defined in the specification of the present invention. Accordingly, all claims patentably

define over the Traw patents and Blumenau. The Examiner is respectfully requested to reconsider

and withdraw the rejection of claim 1-24 under 35 U.S.C. §103.

Conclusion

The present invention is not taught or suggested by the prior art. Accordingly, the

Examiner is respectfully requested to reconsider and withdraw the rejection of the claims. An

early Notice of Allowance is earnestly solicited.

The Commissioner is hereby authorized to charge any fees associated with this

communication to Deposit Account No. 09-0461.

Respectfully submitted

July 30, 2004
Date

Mark D. Simpson, Esquire
Registration No. 32,942

SYNNESTVEDT & LECHNER LLP
2600 ARAMARK Tower
1101 Market Street
Philadelphia, PA 19107

Telephone: (215) 923-4466
Facsimile: (215) 923-2189

M:\MSimpson\Clients\IBM Raleigh RSW\26943 USA\Patent Office\reply to action of 04302004.wpd